Blind Quantum Computing with Weak Coherent Pulses

Blind Quantum Computing with Weak Coherent Pulses

Vedran Dunjko,[1,2] Elham Kashefi,[3] and Anthony Leverrier[4,5]

[1]SUPA, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom
[2]Division of Molecular Biology, Ruđer Bošković Institute, Bijenička cesta 54, P.P. 180, 10002 Zagreb, Croatia
[3]School of Informatics, The University of Edinburgh, Edinburgh EH8 9AB, United Kingdom
[4]ICFO-Institut de Ciencies Fotoniques, Avenida Carl Friedrich Gauss 3, 08860 Castelldefels (Barcelona), Spain
[5]Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland

(Received 4 December 2011; published 18 May 2012)

The universal blind quantum computation (UBQC) protocol [A. Broadbent, J. Fitzsimons, and E. Kashefi, in *Proceedings of the 50th Annual IEEE Symposiumon Foundations of Computer Science* (IEEE Computer Society, Los Alamitos, CA, USA, 2009), pp. 517–526.] allows a client to perform quantum computation on a remote server. In an ideal setting, perfect privacy is guaranteed if the client is capable of producing specific, randomly chosen single qubit states. While from a theoretical point of view, this may constitute the lowest possible quantum requirement, from a pragmatic point of view, generation of such states to be sent along long distances can never be achieved perfectly. We introduce the concept of ϵ blindness for UBQC, in analogy to the concept of ϵ security developed for other cryptographic protocols, allowing us to characterize the robustness and security properties of the protocol under possible imperfections. We also present a remote blind single qubit preparation protocol with weak coherent pulses for the client to prepare, in a delegated fashion, quantum states arbitrarily close to perfect random single qubit states. This allows us to efficiently achieve ϵ-blind UBQC for any $\epsilon > 0$, even if the channel between the client and the server is arbitrarily lossy.

DOI: 10.1103/PhysRevLett.108.200502 PACS numbers: 03.67.Hk, 03.67.Ac, 03.67.Dd, 03.67.Lx

While modern advances in quantum information are making strides towards scalable quantum computers, the dream of small and privately owned quantum computers remains very distant. Realistically, large quantum servers may in the near future take a role similar to that occupied by massive superclusters today. They will be remotely accessed by a large number of clients, using their home-based simple devices, to solve tasks which seem difficult for classical computers, while enjoying full privacy guaranteed by an efficient cryptographic scheme.

Various protocols have been devised with the goal of realizing such delegated, yet private and secure, quantum computing [1–5]. These protocols vary upon their requirements for the client and the achievable level of security. Among them, the universal blind quantum computing (UBQC) proposed by Broadbent, Fitzsimons and Kashefi [1] stands as the optimal one, with the lowest requirements on the client: in particular, no quantum memory is needed. The security offered by the ideal UBQC protocol is unconditional: the server cannot learn anything about the client computation, input or output. This flavor of security is called blindness. The feasibility of UBQC using different physical resources has been addressed [5,6] and the potential of UBQC already has prompted experimental demonstrations on a small scale [7].

The only ''nonclassical'' requirement for the client in the ideal UBQC is that she can prepare single qubits in the state $|+_\theta\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle)$ with $\theta \in \{0, \pi/4, \ldots, 7\pi/4\}$. The blindness of the UBQC protocol has only been established in the ideal case where the client prepares perfect qubits. In any physical implementation, however, the preparation will inevitably be imperfect and this has to be taken into account before making any statement about security. For instance, the qubits could be encoded in the polarization of a single photon generated by a realistic single photon source. Then completely suppressing the probability of inadvertently sending two or more identically polarized photons instead of one is very difficult, yet such an event would invalidate the perfect privacy of the client. While the future may bring scalable and fault-tolerant quantum computation required for the server, perfect quantum devices required to guarantee perfect security for the client are unlikely to ever be achieved in practice.

The main contribution of this Letter is towards this direction: we investigate the security of UBQC with realistic imperfections for the client. For this purpose, we introduce the framework of approximate blindness (ϵ blindness) where the (small) parameter ϵ quantifies the maximal probability of successfully distinguishing between the actual protocol and the ideal one introduced in [1]. A similar approach to defining approximate security has been a milestone in the context of cryptography, and recently extended to the case of quantum key distribution (QKD) [8,9] and other quantum cryptographic primitives in the, so-called, bounded storage and noisy storage models [10–12].

We will show that the level of security is indeed higher when the states prepared by the client are closer to the ideal

qubits. We then introduce a protocol allowing the client to prepare the qubits in a delegated fashion at the server's location. The client needs to encode the quantum information into the polarization of weak coherent pulses which are sent to the server through an arbitrarily lossy quantum channel. Therefore, the burden of preparing very good qubits is put on the server, who needs, in particular, to be able to perform nondemolition quantum measurements [13]. We will show that these realistic requirements (for the client) are compatible with ϵ-blind UBQC, where ϵ can be made arbitrarily small. This approach shares striking similarities with the history of QKD where the initial protocols required true single photons but later became compatible with the much more practical weak coherent pulses.

We begin with a brief recap of the UBQC protocol.

Universal blind quantum computation.—The UBQC protocol is set in the framework of measurement-based quantum computation (MBQC) [14–16]. In MBQC the underlying resource is a multipartite entangled quantum state and the computation is executed by performing measurements on its subsystems. In particular, this resource state can be a generic *brickwork* state, a close relative of the cluster state (see Supplemental Material for details [17]). By applying single qubit measurements parametrized by a measurement angle ϕ from the discrete set $\{0, \pi/4, \ldots, 7\pi/4\}$, which collapse the measured qubit state to one of the two eigenstates $\{|\pm_\phi\rangle = \frac{1}{\sqrt{2}} \times (|0\rangle \pm e^{i\phi}|1\rangle)\}$, with corresponding eigenvalues ± 1, one can achieve universal quantum computation [1]. Here, the computation itself is encoded in the measurement angles alone and the underlying resource is generic.

The classical and quantum part of MBQC can be conceptually separated. One can imagine a classical controller which generates the measurement angles and a quantum unit which prepares the resource state, performs the measurements (as dictated by the controller unit), and returns the measurement outcomes to the controller unit. The outcomes are crucial for the adaptive structure of MBQC: since they are probabilistic, the subsequent measurement angles must depend on them to ensure deterministic computation [18,19].

The central idea behind UBQC is to use this separation and allocate the classical controller unit to the client and the quantum unit to the server. To ensure privacy, however, the computation needs to be encoded: this is achieved in UBQC by effectively encoding the resource state.

The standard procedure for MBQC, to prepare the resource state, is to start with a set of qubits in a fixed state, say $|+\rangle := |+_0\rangle$, and to apply an entangling operation of the controlled phase gate (CTRL-Z) to some of them.

In UBQC, by contrast, the client will provide the initial phase rotated qubits of the form $|+_\theta\rangle$ to the server, without informing him of the values of $\theta \in \{0, \pi/4, \ldots, 7\pi/4\}$. Applying the entangling gates then prepares an encoded resource state. Now, if one was to measure a qubit in the usual MBQC protocol with some measurement angle ϕ, this would be equivalent to measuring the prerotated qubit in the state $|+_\theta\rangle$ with the angle $\delta' = \phi + \theta \bmod 2\pi$, as the phase rotation and CTRL-Z gate commute. In this case, the measurement angle alone says nothing about the computation run, but a malicious server may still try to learn something about θ when given δ', hence also about ϕ (i.e., about the computation).

To solve this security loophole, UBQC exploits the probabilistic nature of MBQC. The client sends a modified measurement angle $\delta = \phi + \theta + r\pi \bmod 2\pi$ where $r \in \{0, 1\}$ is chosen randomly by the client and hidden from the server. The value of r can be interpreted as a flip of the measurement outcome, which can be easily compensated by the client.

Now the quantum information (prerotated qubits) and classical information (measurement angles) accessible to the server are no longer correlated to the client's desired computational angles (denoted ϕ), and this constitutes the crux of the proof of blindness of UBQC [1].

One can summarize the UBQC protocol as follows: Initially, in the preparation phase, the client sends S (the size of the computation) randomly prerotated qubits in the states $\{|+_{\theta_i}\rangle\}_{i=1}^{S}$, to the server, keeping the angles θ_i secret. The server then builds up the brickwork state using the received qubits and the CTRL-Z interaction. Proceeding sequentially on each qubit, if the desired measurement angle for qubit i was ϕ_i (defined for the non-prerotated resource state, and including the necessary adaptations to the angle based on prior measurement outcomes $s_{k<i}$), the client will ask the server to measure the qubit with respect to the angle $\delta_i = \phi_i + \theta_i + r_i\pi \bmod 2\pi$ where the binary parameter r_i is chosen randomly. The server reports each measurement outcome s_i which the client flips if $r_i = 1$.

In the case of an honest server, this procedure yields the correct outcome of the computation. Moreover, regardless of the malicious activity of the server the client's privacy is unconditional—the protocol is blind (see Supplemental Material for details [17]).

This blindness, however, only holds if the client can prepare the needed qubits perfectly. In a practical implementation, imperfection is inevitable and perfect blindness cannot be achieved. For this reason, a notion of approximate blindness is required.

Approximate blindness.—A difficulty in characterizing the UBQC protocol is that it is adaptive. However, as far as blindness is concerned, the reported outcomes s_i of the server do not matter; they only affect the correctness of the protocol [20]. Hence one can assume $s_i = 0$ (i.e., the server measurement always projects into the $+1$ eigenvalue, similar to a post-selection scenario), and since the random parameters r_i can be chosen in advance, the need for the adaptive structure can be ignored. Therefore, blindness can be studied through the following joint state of the client and server:

$$\pi_{AB}^{\text{ideal}} = \frac{1}{2^{4S}} \sum_{\vec{\phi},\vec{r}} \bigotimes_{i\in[S]} \underbrace{|\phi_i\rangle\langle\phi_i| \otimes |r_i\rangle\langle r_i|}_{\text{Client}(A)} \otimes \underbrace{|+_{\theta_i}\rangle\langle+_{\theta_i}| \otimes |\delta_i\rangle\langle\delta_i|}_{\text{Server}(B)},$$

which contains all the relevant information pertaining to the security of a run of a UBQC protocol as seen by the server [21]. In this classical-quantum state, S denotes the overall size of the computation. The client's register contains the user's secret classical information—the computational angles ϕ_i characterizing the desired computation, and the r_i parameters chosen randomly and unknown to the server. The server's register contains quantum information—the qubits in states $|+_{\theta_i}\rangle$ which are sent by the client, as well as the measurement angles δ_i. Note that ϕ_i, r_i and δ_i are all represented by classical, orthogonal states.

If the information shared by the client and the server can be described by the state π_{AB}^{ideal}, then a malicious server cannot learn anything about the computation of the client [1]. Since the security holds for any action of the server, any UBQC protocol described by a state of the form

$$(\mathbb{1}_A \otimes \mathcal{E})\pi_{AB}^{\text{ideal}} \tag{1}$$

for any completely positive trace preserving (CPTP) map $\mathcal{E}$ (representing any possible deviation from the protocol by the server) is equally blind. We refer to such states as unconditionally blind states and define the family $\mathcal{F}$ of such states as follows:

$$\mathcal{F} = \{(\mathbb{1}_A \otimes \mathcal{E})\pi_{AB}^{\text{ideal}} | \mathcal{E} \text{ is a CPTP map}\}. \tag{2}$$

In order to analyze the impact of imperfections caused by a realistic implementation, we consider the settings where the client sends general states ρ^{θ_i} instead of the perfect states $|+_{\theta_i}\rangle$. In this case, the joint state representing all the information exchanged in the protocol is given by:

$$\pi_{AB}^{\{\rho^{\theta_i}\}} = \frac{1}{2^{4S}} \sum_{\vec{\phi},\vec{r}} \bigotimes_{i\in[S]} \underbrace{|\phi_i\rangle\langle\phi_i| \otimes |r_i\rangle\langle r_i|}_{\text{Client}} \otimes \underbrace{\rho^{\theta_i} \otimes |\delta_i\rangle\langle\delta_i|}_{\text{Server}}. \tag{3}$$

We can now introduce the notion of ϵ blindness:

Definition 1.—A UBQC protocol with imperfect client preparation described by the shared joint state $\pi_{AB}^{\{\rho^{\theta_i}\}}$ is ϵ blind if the trace distance between the family of unconditionally blind states and the state $\pi_{AB}^{\{\rho^{\theta_i}\}}$ is less than ϵ:

$$\min_{\pi_{AB}^{\varepsilon}\in\mathcal{F}} \frac{1}{2} \| \pi_{AB}^{\{\rho^{\theta_i}\}} - \pi_{AB}^{\varepsilon} \| \leq \epsilon. \tag{4}$$

Such a notion of security is particularly desirable as it is composable [9,22–24]. One can also extend it to a more general setting considering prior knowledge about the computation (see Supplemental Material [17]).

If the states ρ^{θ_i} generated by the client are uncorrelated (which holds for instance if the process determining the parameters θ_i is random and memoryless), the distance between the perfectly blind state and the approximate state $\pi_{AB}^{\{\rho^{\theta_i}\}}$ can be bounded in terms of the distance between the individual states ρ^{θ_i} and the corresponding perfect qubit states $|+_{\theta_i}\rangle$. In particular, defining

$$\epsilon_{\text{prep}} = \max_{\theta_i} \frac{1}{2} \| \rho^{\theta_i} - \varepsilon(|+_{\theta_i}\rangle\langle+_{\theta_i}|) \| \tag{5}$$

for some CPTP map $\mathcal{E}$ independent of all θ_i, then one can show (see Supplemental Material [17]) that

$$\min_{\pi_{AB}^{\varepsilon}\in\mathcal{F}} \frac{1}{2} \| \pi_{AB}^{\{\rho^{\theta_i}\}} - \pi_{AB}^{\varepsilon} \| \leq S\epsilon_{\text{prep}}. \tag{6}$$

This means that the ability to prepare good approximations of the states $|+_{\theta_i}\rangle$ translates into the ability to perform approximately blind universal quantum computing.

This, however, is not completely satisfying from the client's perspective. Indeed, the client can only achieve a given value of ϵ_{prep} in practice, meaning that for a fixed security parameter ϵ, she cannot perform a computation with more that $\epsilon/\epsilon_{\text{prep}}$ steps. In order to allow for computation of arbitrary size, it is necessary to prepare arbitrary good qubits and the solution is to delegate this task to the server, who is assumed to be much more powerful than the client.

We proceed by presenting such a remote blind qubit state preparation (RBSP) protocol where the client only needs to prepare weak coherent pulses with a given polarization. The requirements for the client are therefore minimal. In particular, they are the same as in most practical implementations of discrete-variable QKD. The difficulty here is transferred to the server who has to perform a quantum nondemolition measurement to obtain the desired qubit. As we will show, using the RBSP protocol S times, the client can reach a joint state $\pi_{AB}^{\{\rho^{\theta_i}\}}$ which is ε close to the family $\mathcal{F}$ of perfectly blind states.

UBQC with remote blind qubit state preparation using weak coherent pulses.—The RBSP protocol is designed to serve as a substitute for the process of sending one individual perfect random qubit which allows for imperfect devices and an imperfect channel.

Ideally, its outcome will satisfy the following properties: (**A**) the state in the server's possession is $\mathcal{E}(|+_\theta\rangle\langle+_\theta|)$ for a CPTP map $\mathcal{E}$, independent of θ known to the client alone—guaranteeing perfect blindness, see Eq. (5); (**B**) the protocol is never aborted in the honest server scenario—guaranteeing robustness of the encompassing UBQC; (**C**) in the honest server scenario, the map $\mathcal{E}$ is the identity—guaranteeing the correctness of the UBQC protocol.

When imperfections are taken into account, the UBQC using RBSP in the preparation phase approaches the properties of blindness and robustness asymptotically. Hence, we are interested in the following properties: ϵ blindness, as described above, and ϵ robustness which guarantees that

the honest abort probability is less than ϵ. Despite the imperfect preparation stage, we also show that the correctness of the protocol holds in the honest scenario, whenever the client does not abort.

To run the RBSP protocol, the client sends a sequence of N weak coherent pulses (small amplitude, phase-randomized coherent states) with random polarization σ in the set $\{0, \pi/4, \ldots, 7\pi/4\}$ to the server. If the transmittance of the channel from the client to the server is supposed to be at least T, then the mean photon number of the source is set to $\mu = T$ [25]. The introduced phase randomization simplifies the security analysis and causes the state emitted from the source to be:

$$\rho^{\sigma} = \sum_{k=0}^{\infty} p_k |k\rangle\langle k|_{\sigma}$$

where $|k\rangle_{\sigma} := |+_{\sigma}\rangle^{\otimes k}$ corresponds to k photons, occurring with probability $p_k = e^{-T}T^k/k!$, with polarization σ. Each pulse is then a probabilistic mixture of Fock states. The Poissonian distribution obtained here is not crucial for the RBSP protocol. For instance, it would work equally well (with readjustment of parameters) with any source realizing a mixture of polarization encoded photon number states, such as polarized thermal states, provided that the probability of getting a single photon is not too small.

The server then performs nondemolition photon number measurements on the pulses he receives, declaring the number outcomes to the client. This additional requirement on the quantum server, while a challenging task has, already been experimentally implemented [26]. At this point, the client checks the number of reported vacuum states—if this number is greater than $N(e^{-T^2} + T^2/6)$, she aborts the protocol. A higher value would be indicative to either a lossier than believed channel, or more importantly, that the server lied in an attempt to cheat.

If the protocol was not aborted, the server performs the interlaced 1D cluster computation (I1DC) subroutine , using the photons obtained by the number measurement of the received coherent pulses. In this subroutine, the server couples the first and the second qubit (i.e., photons) with the interaction CTRL-Z. ($H \otimes \mathbb{1}$), and the first qubit of the pair is then measured in the Pauli X basis and the measurement outcome is sent to the client. The remaining qubit is then coupled to the third qubit in the input set and measured in the same basis. This process is repeated until only one qubit remains unmeasured, in some state $|+_{\theta}\rangle$.

Using her knowledge about the polarizations of each of the pulses initially sent, and the reported binary string of outcomes, the client can compute the angle θ (see Supplemental Material for details [17]). The pair θ (held by the client) and $|+_{\theta}\rangle$ (held by the server), is the required outcome of the RBSP protocol.

The intuition behind this protocol is the following. The I1DC subroutine is such that if the server is totally ignorant about the polarization of at least one photon in the 1D cluster, then he is also totally ignorant about the final angle θ. In order to exploit this property, the client should make sure that the server will at least once measure a single photon and put it in the cluster. The cheating strategy for the server consists in claiming he received 0 photon when he received 1 and claiming he received 1 when he in fact measured several (in which case he can learn something about their polarization). In order to avoid this attack, the client simply verifies that the reported statistics of the server are compatible with the assumed transmittance of the channel. Note that the server cannot learn anything useful, even if he deviates from the prescribed I1DC subroutine, if one of the weak coherent pulses generated one photon, and was declared as such. We now give more quantitative statements which are proven in the Supplemental Material [17] (together with detailed descriptions of both RBSP and I1DC).

For the described RBSP protocol, property (**A**) holds except with probability p_{fail} and properties (**B**) and (**C**) hold except with probability p_{abort}. These probabilities p_{abort} and p_{fail} can be bounded as functions of the transmittance T and the parameter N as follows:

$$p_{\text{fail}}, p_{\text{abort}} \leq \exp\left(-\frac{NT^4}{18}\right). \tag{7}$$

Using the bound on p_{fail}, the trace distance between the perfectly blind qubit state and the state ρ_{θ} generated by RBSP can be bounded as

$$\frac{1}{2} \| \rho^{\theta} - \mathcal{E}(|+_{\theta}\rangle\langle+_{\theta}|) \| \leq p_{\text{fail}}$$

for a fixed CPTP map $\mathcal{E}$ independent of θ. From this, by the criterion given in expression (6), the bound given in Eq. (7) and the union bound, we have that a protocol using the RBSP generated states is ϵ blind with $\epsilon \leq S\exp(-NT^4/18)$, where T is a lower bound on the channel transmittance, and N the number of states used in each instance of RBSP. These results are proven in detail in the Supplemental Material [17] and collected in the following main theorem:

Theorem 1.—A UBQC protocol of computation size S, where the client's preparation phase is replaced with S calls to the coherent state remote blind qubit state preparation protocol, with a lossy channel connecting the client and the server of transmittance no less than T, is correct, ϵ robust and ϵ blind for a chosen $\epsilon > 0$ if the parameter N of each instance of the remote blind qubit state preparation protocol called is chosen as follows:

$$N \geq \frac{18\ln(S/\epsilon)}{T^4}.$$

We acknowledge that the RBSP protocol is not immune to noise in the channel or to significant preparation errors on the side of the client. A method of performing RBSP in a fault-tolerant way, by adapting techniques used to ensure

the fault tolerance of UBQC itself [1,6,27], is under investigation by the authors. However, noise can only jeopardize the correctness of our protocol, but never the guaranteed security levels.

Conclusions and outlook.—In this work we have addressed the security of UBQC under the presence of imperfections through the concept of ϵ blindness. Following this we have given a remote qubit state preparation preprotocol which allows a client, with access to weak coherent pulses only, to enjoy UBQC with arbitrary levels of security.

The transition from the idealized setting of UBQC using single photon qubits to the present protocol using weak coherent pulses brings UBQC significantly closer to real-life applications for, e.g., an unconditionally secure quantum network. The parallel with the evolution of QKD is also very interesting. Note that in QKD, weak coherent pulses were not very attractive for long distance communication before the invention of protocols with decoy states [28]. Indeed, these decoy states made the optimal intensity μ of the attenuated laser be roughly a constant, in contrast with the optimal $\mu \approx T$ without decoy states. In the case of UBQC, it might also be the case that decoy states could improve the optimal value of μ and therefore significantly decrease the required number of weak coherent pulses used in an instance of RBSP for a given computation.

We thank Erika Andersson for insightful discussions. We would also like to acknowledge the hospitality of the Telecom ParisTech Quantum Group where this work was initiated during visits by all the authors. V. D. is supported by EPSRC (Grant No. EP/G009821/1), E. K. is supported by EPSRC (Grant No. EP/E059600/1) and A. L. received financial support from the EU ERC Starting grant PERCENT. This work was done while A. L. was at ICFO.

[1] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *Proceedings of the 50th Annual IEEE Symposiumon Foundations of Computer Science* (IEEE Computer Society, Los Alamitos, CA, USA, 2009), pp. 517–526.
[2] A. Childs, *Quant. Inf. Compt.* (2005), p. 456.
[3] P. Arrighiand and L. Salvail, Int. J. Quantum. Inform. **4**, 883 (2006).
[4] D. Aharonov, M. Ben-Or, and E. Eban, in *Proceedings of Innovations in Computer Science 2010* (Tsinghua University Press, Beijing, China, 2010), p. 453.
[5] T. Morimae, V. Dunjko, and E. Kashefi, arXiv:1009.3486v2.
[6] T. Morimae and K. Fujii, arXiv:1110.5460v1.
[7] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Science **335**, 303 (2012).
[8] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[9] J. Müller-Quade and R. Renner, New J. Phys. **11**, 085006 (2009);.
[10] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, SIAM J. Comput. **37**, 1865 (2008).
[11] R. König, S. Wehner, and J. Wullschleger, IEEE Trans. Inf. Theory **58**, 1962 (2012). .
[12] S. Wehner, C. Schaffner, and B. M. Terhal, Phys. Rev. Lett. **100**, 220502 (2008).
[13] P. Grangier, J. Levenson, and J. Poizat, Nature (London) **396**, 537 (1998).
[14] R. Raussendorf and H. J. Briegel,Phys. Rev. Lett. **86**, 5188 (2001).
[15] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).
[16] R. Jozsa, arXiv:0508124v2.
[17] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.108.200502 for detailed proofs of the claims stated in this Letter, along with a more detailed description of the UBQC protocol.
[18] V. Danos and E. Kashefi, Phys. Rev. A **74**, 052310 (2006).
[19] D. E. Browne, E. Kashefi, M. Mhalla, and S. Perdrix, New J. Phys. **9**, 250 (2007).
[20] After the prerotated qubits have been sent from the client to the server (and θ_i rotations fixed), the possible transcripts of the communication between the client and the server depend on two sequences of parameters: the measurement results s_i sent by the server, and the (random) parameters r_i chosen by the client. The classical information sent by the client depends on $r_i + s_i \bmod 2$ (see step 3.5 of *UBQC protocol* in the Supplemental Material [17]). Since the parameters r_i are random and unknown to the server, so are the values $r_i + s_i \bmod 2$. Hence the responses from the client are independent from the choice of the server's reporting strategy. So we may fix the reporting strategy (and the measurement outcomes) without loss of generality.
[21] The client has also access to the angles θ_i. However, these angles do not constitute the secret the client wishes to hide—for blindness only the r_i parameters and the (adapted) computation angles are relevant. Thus in the presented joint state we explicitly place the client's secret in the client's register, and all information accessible to the server in the server's register.
[22] R. Renner and R. König, in *Theory of Cryptography, Second Theory of Cryptography Conference* (2005), pp. 407–425.
[23] R. König, R. Renner, A. Bariska, and U. Maurer, Phys. Rev. Lett. **98**, 140502 (2007).
[24] M. Ben-or, D. W. Leung, and D. Mayers, in *Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005*, edited by J. Kilian, Lecture Notes in Computer Science Vol. 3378 (Springer-Verlag, Berlin, 2005), pp. 386–406.
[25] This value of $\mu = T$ is optimal for our security analysis; however, other values are in principle admissible as well.
[26] C. Guerlin, J. Bernu, S. Deleglise, C. Sayrin, S. Gleyzes, S. Kuhr, M. Brune, J.-M. Raimond, and S. Haroche, Nature (London) **448**, 889 (2007).
[27] R. Raussendorf, J. Harrington, and K. Goyal, New J. Phys. **9**, 199 (2007).
[28] H. K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).